This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans. **Updates to items appearing in previous bulletins are listed in bold text.** The text in the Risk column appears in red for vulnerabilities ranking High. The risks levels applied to vulnerabilities in the Cyber Security Bulletin are based on how the "system" may be impacted. The Recent Exploit/Technique table contains a "Workaround or Patch Available" column that indicates whether a workaround or patch has been published for the vulnerability which the script exploits.

- Astaro Security Linux System Information Disclosure
- **Caolan McNamara & Dom Lachowicz Wvware Buffer Overflow (Updated)**
- Bogofilter EMail Filter Remote Denial of Service
- **Gaim Buffer Overflows in Processing MSN Protocol (Updated)**
- **GD Graphics Library Remote Integer Overflow (Updated)**
- Gentoo Gentoolkit 'qpkg' Elevated Privileges
- Gentoo Portage 'dispatch-conf' Elevated Privileges
- **GNU Troff (Groff) Insecure Temporary File Creation (Updated)**
- Haserl Environment Variable Manipulation
- HP OpenView Operations Remote Privilege Escalation
- **ImageMagick Remote EXIF Parsing Buffer Overflow (Updated)**
- Info-ZIP Zip Remote Recursive Directory Compression Buffer Overflow
- ISC DHCPD Package Remote Format String
- **Larry Wall Perl Insecure Temporary File Creation (Updated)**
- **LibTIFF Buffer Overflows (Updated)**
- Multiple Vendors IpTables Initialization Failure
- **Multiple Vendors RSync Path Validation (Updated)**
- **Multiple Vendors Rsync Input Validation Error in sanitize_path() May Let Remote Users Read or Write Arbitrary Files (Updated)**
- **Multiple Vendors Gaim MSNSLP Remote Buffer Overflow (Updated)**
- **Multiple Vendors Linux Kernel IPTables Logging Rules Remote Denial of Service (Updated)**
- **Multiple Vendors LinuxPrinting.org Foomatic-Filter Arbitrary Code Execution (Updated)**
- **Multiple Vendors Trustix LVM Utilities Insecure Temporary File Creation (Updated)**
- **Multiple Vendors LibXpm Image Decoding Multiple Remote Buffer Overflow (Updated)**
- **MySQL Mysql_real_connect Function Remote Buffer Overflow (Updated)**
- **MySQL 'Mysqlhotcopy' Script Elevated Privileges (Updated)**
- **MySQL Security Restriction Bypass & Remote Denial of Service (Updated)**
- **NetaTalk Insecure Temporary File Creation (Updated)**
- PostgreSQL Unspecified RPM Initialization Script
- Proxytunnel Remote Format String
- **QwikMail Format String (Updated)**
- **Rob Flynn Gaim Multiple Vulnerabilities (Updated)**
- Sophos MailMonitor SMTP Email Handling
- SpamAssassin Remote Denial of Service
- **Squid Proxy NTLM Buffer Overflow (Updated)**
- **Squid Remote Denial of Service (Updated)**

    - **Squid Proxy NTLM Authentication Remote Denial of Service (Updated)**
    - **Subversion Mod_Authz_Svn Metadata Information Disclosure (Updated)**
    - Technote 'main.cgi' Input Validation
    - **Tomasz Kloczko Shadow Authentication Bypass (Updated)**
    - **xmlsoft Libxml2 Multiple Remote Stack Buffer Overflows (Updated)**
    - yChat HTTP Remote Denial of Service
    - Yukihiro Matsumoto Ruby Infinite Loop Remote Denial of Service
    - Zile Buffer Overflows
- Multiple Operating Systems
    - AntiBoard Input Validation
    - **Cisco Systems Cisco IOS Telnet Service Remote Denial of Service (Updated)**
    - eGroupWare JiNN Directory Traversal
    - Gallery Cross-Site Scripting
    - FsPHPGallery Multiple Input Validation
    - Gbook MX Multiple Unspecified SQL Injection
    - Goollery Multiple Cross-Site Scripting
    - Moodle Remote Glossary Module SQL Injection
    - **Multiple Vendor Anti-Virus Software Detection Evasion (Updated)**
    - **Multiple Web Browsers TABLE Elements Interpretation (Updated)**
    - **Multiple Web Browsers Font Tag Denial of Service (Updated)**
    - NetGear ProSafe Dual Band Wireless VPN Firewall Default SNMP Community String
    - Paystream AudienceConnect SecureEditor Unauthorized Access
    - Pierre Chifflier wzdftpd ident Processing Remote Denial of Service
    - Sun Java System Web & Application Servers Remote Denial of Service
    - Sun Java System Application Server HTTP TRACE Information Disclosure

Recent Exploit Scripts/Techniques

Trends

Viruses/Trojans

Bugs, Holes, & Patches

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the

section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the Multiple Operating Systems section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

The Risk levels defined below are based on how the system may be impacted:

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.
- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Windows Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
ArGo Software Design ArGoSoft FTP Server 1.4.x	A vulnerability with an unknown impact exists due to an error which allows shortcut ('.lnk') files to be uploaded. Update to version 1.4.2.2: http://www.argosoft.com/ftpserver/download.aspx We are not aware of any exploits for this vulnerability.	ArGoSoft FTP Server Shortcut Upload	Not Specified	Secunia Advisory ID, SA13063, November 2, 2004
Cisco Cisco Secure Access Control Server 3.3.1	A vulnerability exists in the processing of EAP-TLS authentication data that could permit a remote malicious user to gain access to the network. A remote user can supply a certificate that is cryptographically correct (i.e., with all the proper fields and information) and has a valid username to gain access to the network, even if the certificate is not signed by a trusted authority. The vendor has issued a fixed version (3.3.2). Users can upgrade or can replace the current CSCRL.dll Windows Dynamic Link Library (DLL) in the Windows System32 folder with a fixed DLL and restart Cisco Secure ACS for Windows. Replacing the DLL fixes the problem and does not require a full upgrade. Upgrades available at: www.cisco.com/warp/public/707/cisco-sa-20041102-acs-eap-tls.shtml There is no exploit code required.	Cisco Secure Access Control Server EAP-TLS Authentication	Medium	SecurityTracker Alert ID, 1012046, November 2, 2004

IceWarp Merak Mail Server 7.5.2 and 7.6.0 with Icewarp Web Mail	Multiple vulnerabilities exist in Merak Mail Server with IceWarp Web Mail. A remote malicious user can conduct cross-site scripting attacks and a remote authenticated user can rename and delete files on the target system. Among other errors, several scripts do not properly validate user-supplied input, including send.html, attachment.html, and folderitem.html. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	IceWarp Merak Mail Server Multiple Remote Vulnerabilities	Medium	SecurityTracker Alert ID, 1012099, November 5, 2004
Kerio Technologies Inc. Kerio Personal Firewall 4.1.2 and prior	A vulnerability exists that could permit a remote malicious user to cause Denial of Service conditions. There is a packet processing flaw that can trigger 100% CPU utilization on the target system. The vendor has issued a fixed version (4.1.2), available at: http://www.kerio.com/kpf_download.html A Proof of Concept exploit has been published.	Kerio Personal Firewall Remote Denial of Service	Low	SecurityTracker Alert ID, 1012116, November 8, 2004
Microsoft ISA Server 2000, Proxy Server 2.0	A spoofing vulnerability exists that could enable a malicious user to spoof trusted Internet content. Users could believe they are accessing trusted Internet content when in reality they are accessing malicious Internet content, for example a malicious web site. Updates available at: http://www.microsoft.com/technet/security/bulletin/ms04-039.mspx We are not aware of any exploits for this vulnerability.	Microsoft Servers Spoofing CVE Name: CAN-2004-0892	Low	Microsoft Security Bulletin, MS04-039, November 9, 2004

Microsoft Internet Explorer 6.0 SP1, Microsoft Internet Explorer 6.0	A remote buffer overflow vulnerability exists due to insufficient boundary checks performed by the application and results in a Denial of Service condition. Arbitrary code execution may be possible as well. No workaround or patch available at time of publishing. **An exploit script has been published.**	Microsoft Internet Explorer Malformed IFRAME Remote Buffer Overflow	Low/High (High if arbitrary code can be executed)	SecurityFocus, Bugtraq ID 11515, October 25, 2004 **Packetstorm, November 4, 2004**
Microsoft Internet Explorer 6	Two vulnerabilities exist in Internet Explorer, which can be exploited by malicious users to compromise a user's system, link to local resources, and bypass a security feature in Microsoft Windows XP SP2.The two vulnerabilities in combination with actions in the ActiveX Data Object (ADO) model can write arbitrary files can be exploited to compromise a user's system. Microsoft advises customers who have applied the latest Internet Explorer update, MS04-038, to set the 'Drag and Drop or copy and paste files' option in the Internet and Intranet zone to 'Disable' or 'Prompt.' No patch is currently available. **Additional Proof of Concept exploits have been published.**	Microsoft Internet Explorer Two Vulnerabilities CVE Names: CAN-2004-0979 CAN-2004-0727	High	Secunia Advisory,: SA12889, October 20, 2004 US-CERT Vulnerability Note #630720, October 22, 2004 US-CERT Vulnerability Note #207264, October 19, 2004 **SecurityFocus Bugtraq ID: 11467, November 1, 2004**

Microsoft Internet Explorer	Microsoft Internet Explorer does not properly display the location of HTML documents in the status bar. A malicious user could exploit this behavior to mislead users into revealing sensitive information. A vulnerability exists in the way Microsoft Internet Explorer interprets HTML to determine the correct URL to display in the browser's status bar. There is no complete solution to this problem. Install Windows XP Service Pack 2 (SP2). Microsoft Windows XP SP2 does not appear to be affected by this vulnerability. A Proof of Concept exploit has been published.	Microsoft Internet Explorer IFRAME Elements Interpretation	Medium	US-CERT Vulnerability Note VU#960454, November 4, 2004
Microsoft Internet Explorer	Microsoft Internet Explorer (IE) contains a buffer overflow vulnerability that can be exploited to execute arbitrary code with the privileges of the user running IE. A heap buffer overflow vulnerability exists in the way IE handles the SRC and NAME attributes of FRAME, IFRAME and EMBED elements. There is no complete solution to this problem. Install Windows XP Service Pack 2 (SP2). Microsoft Windows XP SP2 does not appear to be affected by this vulnerability. A Proof of Concept exploit has been published.	Microsoft Internet Explorer FRAME, IFRAME, and EMBED Elements Buffer Overflow	High	US-CERT Vulnerability Note VU#842160, November 9, 2004

Microsoft Windows 2000 Advanced Server, Windows 2000 Datacenter Server, Windows 2000 Professional, Windows 2000 Server, Windows XP Home Edition, Windows XP Professional, Windows Server 2003 Datacenter Edition, Windows Server 2003 Enterprise Edition, Windows Server 2003 Standard Edition, Windows Server 2003 Web Edition, Internet Information Services 5.0, Internet Information Services 5.1, Internet Information Services 6.0; Avaya DefinityOne Media Servers, IP600 Media Servers, Modular Messaging (MSS) 1.1, (MSS) 2.0, S3400 Message Application Server, S8100 Media Servers	A Denial of Service vulnerability exists that could allow a malicious user to send a specially crafted WebDAV request to a server that is running IIS and WebDAV. A malicious user could cause WebDAV to consume all available memory and CPU time on an affected server. The IIS service would have to be restarted to restore functionality. Updates available at: http://www.microsoft.com/technet/security/bulletin/MS04-030.mspx Avaya customers are advised to follow Microsoft's guidance for applying patches.http://support.avaya.com/japple/css/japple?temp.groupID=128450&temp.selectedFamily=128451&temp.selectedProduct=154235&temp.selectedBucket=126655&temp.feedbackState=askForFeedback&temp.documentID=203487&PAGE=avaya.css.CSSLvl1Detail&executeTransaction=avaya.css.UsageUpdate() **Additional exploit scripts has been published.**	Microsoft WebDav XML Message Handler Denial of Service CVE Name: CAN-2004-0718	Low	Microsoft Security Bulletin, MS04-030, October 12, 2004 US-CERT Cyber Security Alert SA04-286A, October 12, 2004 SecurityFocus, October 20, 2004 **SecurityFocus, November 2, 2004**

minihttpserver Forum Web Server 2.0	Two vulnerabilities exist which can be exploited to disclose sensitive information. An input validation error makes it possible for malicious people to access arbitrary files outside the web root via directory traversal attacks. User credentials are stored in clear text in the "Username.ini" file, which is readable by any local user on the system. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	minihttpserver Forum Web Server Directory Traversal & Clear Text Disclosure	Medium	Secunia Advisory, SA13078, November 3, 2004
Nortel Nortel Contivity Multi-OS VPN Client 4.91	A vulnerability exists in Nortel Contivity VPN Client, potentially allowing malicious users to open a VPN tunnel to the client. When the Contivity VPN Client establishes a connection to a gateway, the gateway certificate isn't checked before the user answers a dialog box. While the dialog box is displayed to the user, the VPN tunnel remains open allowing the gateway network access to the client system. **Nortel reports that this issue is resolved in Contivity VPN Client for Windows versions V5.01_030 and later. Updates available at: http://www130.nortelnetworks.com/cgi-bin/eserv/cs/main.jsp?BV_SessionID=@@@@1188915395.1099930975@@@@&BV_EngineID=hadcllkimkfdbhkcginchgcgjg.0&level=1&category=10&subcategory=&subtype=&sortField=&sortDir=&viewOptSelect=&viewOpt1=&tranProduct=10621** We are not aware of any exploits for this vulnerability.	Nortel Contivity VPN Client Open Tunnel Certificate Verification	Medium	Secunia Advisory, SA12881, October 20, 2004 **US-CERT Vulnerability Note VU#830214, November 8, 2004**

RARlabs WinRAR 3.40 and prior	A vulnerability exists which can be exploited by malicious people to compromise a user's system. The vulnerability is caused due to an error in the 'Repair Archive' feature. Update to version 3.41: http://www.rarlabs.com/download.htm We are not aware of any exploits for this vulnerability.	RARlabs WinRAR 'Repair Archive' Feature Compromise	Medium	NGS Research, November 2, 2004
Software602 602LAN SUITE 2004.0.04.0909 and prior versions	A vulnerability exists that could permit a remote malicious user to cause a Denial of Service. A remote user can submit an HTTP POST request with a specially crafted Content-Length value and then close the connection before sending the specified amount of data to consume excessive CPU and memory resources on the target system. Upgrade to version 2004.0.04.1104 at: http://www.software602.com/ A Proof of Concept exploit script has been published.	Software602 602LAN SUITE Remote Denial of Service	Low	SecurityFocus, Bugtraq ID, 11615, November 6, 2004
Sourceforge.net MiniShare Buffer 1.4.1 and prior	A buffer overflow vulnerability exists that could allow a remote malicious user to execute arbitrary code on the target system. A remote user can submit a specially crafted, long HTTP GET request to trigger the overflow and execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Sourceforge.net MiniShare Buffer Overflow	High	SecurityTracker Alert ID, 1012106, November 7, 2004

Symantec Norton Anti-Virus 2004, 2005	A vulnerability was reported in Norton Anti-Virus in the script blocking feature. A remote user can create specially crafted scripting code to bypass the security mechanisms and take malicious actions on the target user's system. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Symantec Norton Anti-Virus Script Blocking Bypass	Medium	SecurityTracker Alert ID, 1012079, November 4, 2004
Symantec Symantec LiveUpdate 1.80.19.0, 2.5.56.0	A vulnerability exists which may allow a malicious user to cause Denial of Service conditions in certain cases. Tithe LiveUpdate decompression routine does not check for uncompressed file sizes before attempting to decompress a downloaded LiveUpdate zip file and does not properly validate directory names before creating the directories on the target system. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Symantec LiveUpdate Zip Decompression Routine Denial of Service	Low	SecurityTracker Alert ID, 1012095, November 5, 2004
TIPPS MailPost 5.1.1	Multiple vulnerabilities exist which can be exploited by malicious people to disclose some system information and conduct cross-site scripting attacks. Vulnerabilities are due to input validation errors in 'mailpost.exe' and due to improper behavior in 'mailpost.exe' when supplying a specially crafted '*debug*' parameter. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	TIPPS MailPost Multiple Vulnerabilities	Medium/ High (High if arbitrary code can be executed)	US-CERT VU#596046, VU#107998, VU#306086, VU#858726, November 3, 2004

Touchdown Entertainment LithTech Engine	A format string vulnerability exists in the LithTech Engine, used by many game software titles that could allow a remote malicious user to crash the game server. The method required to trigger the format string flaw may vary, depending on the game software using the engine. In some cases, authentication is required. Many games are affected, including the following: Alien vs Predator 2 v 1.0.9.6 and prior Blood 2 v 2.1 and prior Contract Jack v 1.1 and prior Global Operations v 2.0/2.1 and prior Kiss Psycho Circus v 1.13 and prior Legends of Might and Magic v 1.1 and prior No one lives forever v 1.004 and prior No one lives forever 2 v 1.3 and prior Purge Jihad v 2.2.1 and prior Sanity v 1.0? and prior Shogo v 2.2 and prior Tron 2.0 v 1.042 and prior Of the affected games, Pure Jihad has implemented a fix in version 2.2.2. No solution is available for the the other games. A Proof of Concept exploit has been published.	Touchdown LithTech Engine Format String	Low	SecurityTracker Alert ID, 1012098, November 5, 2004

Trend Micro ScanMail	A vulnerability exists that could allow a remote malicious user to obtain potentially sensitive information or disable the anti-virus protection. A remote user may be able to access the 'smency.nsf' file to disable the anti-virus protection. The remote user may also be able to access other potentially sensitive files, including smconf.nsf, smhelp.nsf, and smadmr5.nsf. No workaround or patch available at time of publishing. We are not aware of any exploits for this vulnerability.	Trend Micro ScanMail Sensitive File Disclosure CVE Name: CAN-2004-1003	Medium	SecurityTracker Alert ID, 1012082, November 4, 2004
WebHost Automation HELM Web Hosting Control Panel 3.1.19 and prior	Two input validation vulnerabilities exist in Helm Web Hosting Control Panel, which can be exploited by malicious people to conduct SQL injection and script insertion attacks. Helm fails to verify input passed to the 'messageToUserAccNum' parameter in the 'compose message' form. Also, input passed to the 'Subject' field in the 'compose message' form is not properly sanitized before being used. Update to version 3.1.20: http://helm.webhostautomation.com/downloads.aspx?product=Helm&menustartnode=Helm%20Control%20Panel A Proof of Concept exploit has been published.	WebHost Automation HELM SQL injection & Cross-Site Scripting	High	Hat-Squad Advisory, November 2, 2004

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
Alvaro Lopez Ortega Cherokee HTTPD 0.1, 0.1.5, 0.1.6, 0.2, 0.2.5-0.2.7, 0.4.6-0.4.8, 0.4.17	A format string vulnerability exists in the 'cherokee_logger_ncsa_write_string()' function due to insufficient sanitization, which could let a remote malicious user execute arbitrary code. Update available at: ftp://alobbs.com/cherokee/0.4/0.4.17/cherokee-0.4.17.1.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200411-02.xml We are not aware of any exploits for this vulnerability.	Cherokee HTTPD Auth_Pam Authentication Remote Format String	High	Gentoo Linux Security Advisory, GLSA 200411-02, November 1, 2004
Apache Software Foundation	A remote Denial of Service vulnerability exists when a malicious user submits multiple specially crafted HTTP GET requests that contain spaces. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Apache Web Server Remote Denial of Service CVE Name: CAN-2004-0942	Low	SecurityTracker Alert ID, 1012083, November 4, 2004

Apache Software Foundation Apache 2.0.35-2.0.52	A vulnerability exists when the 'SSLCipherSuite' directive is used in a directory or location context to require a restricted set of cipher suites, which could let a remote malicious user bypass security policies and obtain sensitive information. OpenPKG: ftp://ftp.openpkg.org/release/ Gentoo: http://security.gentoo.org/glsa/glsa-200410-21.xml Slackware: ftp://ftp.slackware.com/pub/slackware/ **Conectiva: ftp://atualizacoes.conectiva.com.br/10/** **Mandrake: http://www.mandrakesoft.com/security/advisories** There is no exploit code required.	Apache mod_ssl SSLCipherSuite Access Validation CVE Name: CAN-2004-0885	Medium	OpenPKG Security Advisory, OpenPKG-SA-2004.044, October 15, 2004 Gentoo Linux Security Advisory, GLSA 200410-21, October 22, 2004 Slackware Security Advisory, SSA:2004-299-01, October 26, 2004 **Mandrakelinux Security Update Advisory, MDKSA-2004:122, November 2, 2004** **Conectiva Linux Security Announcement, CLA-2004:885, November 4, 2004**

Apache Software Foundation Conectiva Gentoo HP Immunix Mandrake OpenBSD OpenPKG RedHat SGI Trustix Apache 1.3.26-1.3.29, 1.3.31; OpenBSD – current, 3.4, 3.5	A buffer overflow vulnerability exists in Apache mod_proxy when a 'ContentLength:' header is submitted that contains a large negative value, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code. Patches available at: http://marc.theaimsgroup.com/?l=apache-httpd-dev&m=108687304202140&q=p3 OpenBSD: ftp://ftp.openbsd.org/pub/OpenBSD/patches/ OpenPKG: ftp://ftp.openpkg.org/release/2.0/UPD/apache-1.3.29-2.0.3.src.rpm Gentoo: http://security.gentoo.org/glsa/glsa-200406-16.xml Mandrake: http://www.mandrakesoft.com/security/advisories SGI: ftp://patches.sgi.com/support/free/security/ Fedora Legacy: http://download.fedoralegacy.org/redhat/ Slackware: ftp://ftp.slackware.com/pub/slackware/ **Trustix: http://http.trustix.org/pub/trustix/updates/** Currently we are not aware of any exploits for this vulnerability.	Apache Mod_Proxy Remote Buffer Overflow CVE Name: CAN-2004-0492	Low/High (High if arbitrary code can be executed)	SecurityTracker Alert, 1010462, June 10, 2004 Gentoo Linux Security Advisory, GLSA 200406-16, June 22, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:065, June 29, 2004 OpenPKG Security Advisory, OpenPKG-SA-2004.029, June 11, 2004 SGI Security Advisory, 20040605-01-U, June 21, 2004 Fedora Legacy Update Advisory, FLSA:1737, October 14, 2004 US-Cert Vulnerability Note

Apache Software Foundation Apache 1.3, 1.3.1, 1.3.3, 1.3.4, 1.3.46, 1.3.7 -dev, 1.3.9, 1.3.11, 1.3.12, 1.3.14, 1.3.17-1.3.20, 1.3.22-1.3.29, 1.3.31	A buffer overflow vulnerability exists in the 'get_tag()' function, which could let a malicious user execute arbitrary code. **Gentoo:** **http://security.gentoo.org/glsa/glsa-200411-03.xml** **Slackware: ftp://ftp.slackware.com/pub/slackware/s** **Trustix: http://http.trustix.org/pub/trustix/updates/** Exploit scripts have been published.	Apache mod_include Buffer Overflow CVE Name: CAN-2004-0940	High	SecurityFocus, October 20, 2004 **Slackware Security Advisory, SA:2004-305-01, November 1, 2004** **Gentoo Linux Security Advisory, GLSA 200411-03, November 2, 2004** **Trustix Secure Linux Security Advisory, TSLSA-2004-0056, November 5, 2004**

Astaro Astaro Security Linux 4	Several vulnerabilities exist: a vulnerability exists in the PPTP server, which could let a remote malicious user obtain sensitive information; and a vulnerability exists because the firewall incorrectly responds to 'SYN-FIN' packets, which could let a remote malicious user obtain sensitive information. The vendor has issued a new version (4.024), available via Up2Date. Currently we are not aware of any exploits for these vulnerabilities.	Astaro Security Linux System Information Disclosures	Medium	Secunia Advisory, SA13089, November 4, 2004

Caolan McNamara & Dom Lachowicz wvWare version 0.7.4, 0.7.5, 0.7.6 and 1.0.0	A buffer overflow vulnerability exists in the 'strcat()' function call due to the insecure bounds checking, which could let a remote malicious user execute arbitrary code. Updates available at: http://www.abisource.com/bonsai/cvsview2.cgi?diff_mode=context&whitespace_mode=show&root=/cvsroot&subdir=wv&command=DIFF_FRAMESET&root=/cvsroot&file=field.c&rev1=1.19&rev2=1.20 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200407-11.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Conectiva: ftp://atualizacoes.conectiva.com.br/ Debian: http://security.debian.org/pool/updates/main/w/wv/ A Proof of Concept exploit has been published.	wvWare Library Buffer Overflow CVE Name: CAN-2004-0645	High	Securiteam, July 11, 2004 iDEFENSE Security Advisory, July 9, 2004 Conectiva Linux Security Announcement, CLA-2004:863, September 10, 2004 Debian Security Advisory, DSA 550-1, September 20, 2004 **Debian Security Advisory, DSA 579-1, November 1, 2004**

Eric S. Raymond Email Filter 0.9 .0.5, 0.9 .0.4, 0.9 .0.3, 0.92, 0.92.4, 0.92.6, 0.92.7	A remote Denial of Service vulnerability exists in 'quoted-printable decoder' due to a failure to handle malformed email headers. Upgrades available at: http://sourceforge.net/project/showfiles.php?group_id=62265 There is no exploit code required; however, a Proof of Concept exploit has been published.	Bogofilter EMail Filter Remote Denial of Service CVE Name: CAN-2004-1007	Low	Securiteam, November 3, 2004

Gaim Gentoo	Multiple vulnerabilities were reported in Gaim in the processing of the MSN protocol. A remote user may be able to execute arbitrary code on the target system. Several remotely exploitable buffer overflows were reported in the MSN protocol parsing functions. Gentoo: http://security.gentoo.org/glsa/glsa-200408-12.xml SuSE: http://www.suse.de/de/security/2004_25_gaim.html Mandrake: http://www.mandrakesecure.net/en/ftp.php Rob Flynn: http://sourceforge.net/project/showfiles.php?group_id=235&package_id=253&release_id=263425 Slackware: ftp://ftp.slackware.com/pub/slackware/slackware-9.1/patches/packages/gaim-0.82-i486-1.tgz Fedora Legacy: http://download.fedoralegacy.org/redhat/ **Conectiva: ftp://atualizacoes.conectiva.com.br/10/** We are not aware of any exploits for this vulnerability.	Gaim Buffer Overflows in Processing MSN Protocol CVE Name: CAN-2004-0500	High	SecurityTracker, 1010872, August 5, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:081, August 13, 2004 Slackware Security Advisory, SSA:2004-239-01, August 26, 2004 Fedora Legacy Update Advisory, FLSA:1237, October 16, 2004 **Conectiva Linux Security Announcement, CLA-2004:885, November 4, 2004**

GD Graphics Library gdlib 2.0.23, 2.0.26-2.0.28	A vulnerability exists in the 'gdImageCreateFromPngCtx()' function when processing PNG images due to insufficient sanity checking on size values, which could let a remote malicious user execute arbitrary code. OpenPKG: ftp://ftp.openpkg.org/release/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/libg/libgd2/ **Gentoo: http://security.gentoo.org/glsa/glsa-200411-08.xml** An exploit script has been published.	GD Graphics Library Remote Integer Overflow CVE Name: CAN-2004-0990	High	Secunia Advisory, SA12996, October 28, 2004 **Gentoo Linux Security Advisory, GLSA 200411-08, November 3, 2004**
Gentoo Linux 0.2.0_pre10 & prior versions	A vulnerability exists in the 'qpkg' Gentoolkit due to the insecure creation of temporary files, which could let a malicious user obtain elevated privileges. Update available at: http://security.gentoo.org/glsa/glsa-200411-13.xml Currently we are not aware of any exploits for this vulnerability.	Gentoo Gentoolkit 'qpkg' Elevated Privileges	Medium/ High (High if root access can be obtained)	Gentoo Linux Security Advisory GLSA 200411-13:01, November 7, 2004

Gentoo Linux 2.0.51-r2 & prior versions	A vulnerability exists in 'dispatch_conf' due to the insecure creation of temporary files, which could let a malicious user obtain elevated privileges. Update available at: http://security.gentoo.org/glsa/glsa-200411-13.xml Currently we are not aware of any exploits for this vulnerability.	Gentoo Portage 'dispatch-conf' Elevated Privileges	Medium/ High (High if root access can be obtained)	Gentoo Linux Security Advisory GLSA 200411-13:01, November 7, 2004
GNU groff 1.19	A vulnerability exists due to the insecure creation of temporary files, which could possibly let a malicious user overwrite arbitrary files. Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/groff/ **Gentoo: http://security.gentoo.org/glsa/glsa-200411-15.xml** There is no exploit code required.	GNU Troff (Groff) Insecure Temporary File Creation CVE Name: CAN-2004-0969	Medium	Trustix Secure Linux Bugfix Advisory, TSL-2004-0050, September 30, 2004 Ubuntu Security Notice USN-13-1, November 1, 2004 **Gentoo Linux Security Advisory, GLSA 200411-15, November 8, 2 004**

Haserl Haserl 0.4-0.4.2, 0.5, 0.5.1	A vulnerability exists due to a design error that allows the manipulation of environment variables, which could let a remote malicious user manipulate information. Upgrades available at: http://prdownloads.sourceforge.net/haserl/haserl-0.6.0.tar.gz?download There is no exploit code required.	Haserl Environment Variable Manipulation	Medium	Secunia Advisory, SA13031, November 1, 2004
Hewlett Packard Company OpenView Operations for HP-UX 6.0, 7.0, 8.0, OpenView Operations for Solaris 6.0, 7.0, 8.0	A vulnerability exists which could let a remote authenticated malicious user obtain elevated privileges. Patches available at: http://itrc.hp.com/ We are not aware of any exploits for this vulnerability.	HP OpenView Operations Remote Privilege Escalation	Medium	HP Security Bulletin, HPSBMA01092, November 2, 2004

ImageMagick ImageMagick 5.3.3, 5.4.3, 5.4.4.5, 5.4.7, 5.4.8 .2-1.1.0, 5.4.8, 5.5.3 .2-1.2.0, 5.5.6 .0-20030409, 5.5.7, 6.0, 6.0.1, 6.0.3-6.0.8	A buffer overflow vulnerability exists in the 'EXIF' parsing routine due to a boundary error, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://sourceforge.net/project/showfiles.php?group_id=24099 Redhat: http://rhn.redhat.com/errata/RHSA-2004-480.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/i/imagemagick/ **Gentoo: http://security.gentoo.org/glsa/glsa-200411-11.xml** We are not aware of any exploits for this vulnerability.	ImageMagick Remote EXIF Parsing Buffer Overflow CVE Name: CAN-2004-0981	High	SecurityTracker Alert ID, 1011946, October 26, 2004 **Gentoo Linux Security Advisory, GLSA 200411-11:01, November 6, 2004**
Info-ZIP Zip 2.3	A buffer overflow vulnerability exists due to a boundary error when doing recursive compression of directories with 'zip,' which could let a remote malicious user execute arbitrary code. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/z/zip/zip_2.30-6ubuntu0.1_amd64.deb We are not aware of any exploits for this vulnerability.	Info-ZIP Zip Remote Recursive Directory Compression Buffer Overflow CVE Name: CAN-2004-1010	High	Bugtraq, November 3, 2004 Ubuntu Security Notice, USN-18-1, November 5, 2004

ISC DHCPD 2.0.pl5	A format string vulnerability exists because user-supplied data is logged in an unsafe fashion, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://security.debian.org/pool/updates/main/d/dhcp/ We are not aware of any exploits for this vulnerability.	ISC DHCPD Package Remote Format String CVE Name: CAN-2004-1006	High	Debian Security Advisory, DSA 584-1, November 4, 2004
Larry Wall Perl 5.8.3	A vulnerability exists due to the insecure creation of temporary files, which could possibly let a malicious user overwrite arbitrary files. Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/p/perl/** There is no exploit code required.	Perl Insecure Temporary File Creation CVE Name: CAN-2004-0976	Medium	Trustix Secure Linux Bugfix Advisory, TSL-2004-0050, September 30, 2004 **Ubuntu Security Notice, USN-16-1, November 3, 2004**

libtiff.org LibTIFF 3.6.1	Several buffer overflow vulnerabilities exist: a vulnerability exists because a specially crafted image file can be created, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; a remote Denial of Service vulnerability exists in 'libtiff/tif_dirread.c' due to a division by zero error; and a vulnerability exists in the 'tif_next.c,' 'tif_thunder.c,' and 'tif_luv.c' RLE decoding routines, which could let a remote malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/t/tiff/ Gentoo: http://security.gentoo.org/glsa/glsa-200410-11.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ OpenPKG: ftp://ftp.openpkg.org/release/ Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Mandrake: http://www.mandrakesecure.net/en/ftp.php SuSE: ftp://ftp.suse.com/pub/suse/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-577.html **Slackware: ftp://ftp.slackware.com/pub/slackware/** Proofs of Concept exploits have been published.	LibTIFF Buffer Overflows CVE Name: CAN-2004-0803 CAN-2004-0804 CAN-2004-0886	Low/High (High if arbitrary code can be execute)	Gentoo Linux Security Advisory, GLSA 200410-11, October 13, 2004 Fedora Update Notification, FEDORA-2004-334, October 14, 2004 OpenPKG Security Advisory, OpenPKG-SA-2004.043, October 14, 2004 Debian Security Advisory, DSA 567-1, October 15, 2004 Trustix Secure Linux Security Advisory, TSLSA-2004-0054, October 15, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:109 & MDKSA-

Multiple Vendors Debian Linux 3.0, sparc, s/390, ppc, mipsel, mips, m68k, 0 ia-64, ia-32, hppa, arm, alpha; Linux kernel 2.0.2, 2.4-2.4.26, 2.6-2.6.9	A vulnerability exists in 'iptables.c' and 'ip6tables.c' due to a failure to load the required modules, which could lead to a false sense of security because firewall rules may not always be loaded. Debian: http://security.debian.org/pool/updates/main/i/iptables/iptables_1.2.6a-5.0woody2_sparc.deb Mandrake: http://www.mandrakesecure.net/en/ftp.php There is no exploit code required.	IpTables Initialization Failure CVE Name: CAN-2004-0986	Medium	Debian Security Advisory, DSA 580-1 , November 1, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:125, November 4, 2004

Multiple Vendors Debian Mandrake OpenPKG RedHat SGI Slackware Trustix Debian Linux 3.0, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; rsync 2.3.1, 2.3.2 -1.3, 2.3.2 -1.2, sparc, PPC, m68k, intel, ARM, alpha, 2.3.2, 2.4.0, 2.4.1, 2.4.3- 2.4.6, 2.4.8, 2.5.0-2.5.7, 2.6	A vulnerability exists due to insufficient sanitization of user-supplied path values, which could let a remote malicious user modify system information or obtain unauthorized access. Debian: http://security.debian.org/pool/updates/main/r/rsync Mandrake: http://www.mandrakesecure.net/en/ftp.php Rsync: http://rsync.samba.org/ftp/rsync/rsync-2.6.1.tar.gz Slackware: ftp://ftp.slackware.com/pub/slackware/ Trustix: http://www.trustix.org/errata/misc/2004/TSL-2004-0024-rsync.asc.txt OpenPKG: ftp://ftp.openpkg.org/release/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-192.html SGI: ftp://patches.sgi.com/support/free/security/patches/ProPack/2.4/ Apple: http://www.apple.com/support/security/security_updates.html Fedora Legacy: http://download.fedoralegacy.org/redhat/ **Conectiva: ftp://atualizacoes.conectiva.com.br/** Currently we are not aware of any exploits for this vulnerability.	RSync Path Validation CVE Name: CAN-2004-0426	Medium	Debian Security Advisory, DSA 499-1, May 2, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:042, May 11, 2004 OpenPKG Security Advisory , OpenPKG-SA-2004.025, May 21, 2004 RedHat Security Advisory, RHSA-2004:192-06, May 19, 2004 SGI Security Advisories, 20040508-01-U & 20040509-01, May 28, 2004 Slackware Security Advisory, SSA:2004-124-01, May 3, 2004 Trustix Secure Linux Security Advisory, 2004-

Multiple Vendor Debian SuSE Trustix rsync 2.6.2 and prior	A vulnerability exists in rsync when running in daemon mode with chroot disabled. A remote user may be able read or write files on the target system that are located outside of the module's path. A remote user can supply a specially crafted path to cause the path cleaning function to generate an absolute filename instead of a relative one. The flaw resides in the sanitize_path() function. Updates and patches are available at: http://rsync.samba.org/ SuSE: http://www.suse.de/de/security/2004_26_rsync.html Debian: http://www.debian.org/security/2004/dsa-538 Trustix: http://www.trustix.net/errata/2004/0042/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Mandrake: http://www.mandrakesecure.net/en/ftp.php OpenPKG: ftp://ftp.openpkg.org/release/2.0/UPD/ Tinysofa: http://http.tinysofa.org/pub/tinysofa/updates/server-2.0/i386/tinysofa/rpms.updates/rsync-2.6.2-2ts.i386.rpm TurboLinux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ Fedora Legacy: http://download.fedoralegacy.org/redhat/ **Conectiva: ftp://atualizacoes.conectiva.com.br/** We are not aware of any exploits for this vulnerability.	Rsync Input Validation Error in sanitize_path() May Let Remote Users Read or Write Arbitrary Files CVE Name: CAN-2004-0792	High	SecurityTracker 1010940, August 12, 2004 rsync August 2004 Security Advisory SecurityFocus, September 1, 2004 Fedora Legacy Update Advisory, FLSA:2003, September 30, 2004 **Conectiva Linux Security Announcement, CLA-2004:881, November 1, 2004**

Multiple Vendors Gentoo Linux, 1.4; Rob Flynn Gaim 0.10 x, 0.10.3, 0.50-0.75, 0.78, 0.82, 0.82.1, 1.0, 1.0.1; Slackware Linux -current, 9.0, 9.1, 10.0	A buffer overflow vulnerability exists in the processing of MSNSLP messages due to insufficient verification, which could let a remote malicious user execute arbitrary code. Gentoo: http://security.gentoo.org/glsa/glsa-200410-23.xml Rob Flynn: http://prdownloads.sourceforge.net/gaim/gaim-1.0.2.tar.gz?download RedHat: ftp://updates.redhat.com/ Slackware: ftp://ftp.slackware.com/pub/slackware/slackware-10.0/patches/packages/gaim-1.0.2-i486-1.tgz Ubuntu:http://security.ubuntu.com/ubuntu/pool/main/g/gaim/ **Mandrake: http://www.mandrakesoft.com/security/advisories** We are not aware of any exploits for this vulnerability.	Gaim MSNSLP Remote Buffer Overflow CVE Name: CAN-2004-0891	High	Gentoo Linux Security Advisory, GLSA 200410-23, October 25, 2004 RedHat Security Advisory, RHSA-2004:604-01, October 20, 2004 Slackware Security Advisory, SSA:2004-296-01, October 22, 2004 Ubuntu Security Notice, USN-8-1 October 27, 2004 **Mandrakelinux Security Update Advisory, MDKSA-2004:117, November 1, 2004**

Multiple Vendors Linux kernel 2.6 -test1-test11, 2.6-l 2.6.8; SuSE Linux 9.1	A remote Denial of Service vulnerability exists in the iptables logging rules due to an integer underflow. Update available at: http://kernel.org/ SuSE: ftp://ftp.suse.com/pub/suse/ **A Proof of Concept exploit script has been published.**	Linux Kernel IPTables Logging Rules Remote Denial of Service CVE Name: CAN-2004-0816	Low	SuSE Security Announcement, SUSE-SA:2004:037, October 20, 2004 **Packetstorm, November 5, 2004**

Multiple Vendors LinuxPrinting.org Foomatic-Filters 3.03.0.2, 3.1; Trustix Secure Enterprise Linux 2.0, Secure Linux 2.0, 2.1	A vulnerability exists in the foomatic-rip print filter due to insufficient validation of command-lines and environment variables, which could let a remote malicious user execute arbitrary commands. Mandrake: http://www.mandrakesecure.net/en/ftp.php SuSE: ftp://ftp.suse.com/pub/suse Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Gentoo: http://security.gentoo.org/glsa/glsa-200409-24.xml Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57646-1&searchclause= Conectiva: ftp://atualizacoes.conectiva.com.br/ **Fedora Legacy: http://download.fedoralegacy.org/fedora/1/updates/** We are not aware of any exploits for this vulnerability.	LinuxPrinting.org Foomatic-Filter Arbitrary Code Execution CVE Name: CAN-2004-0801	High	Secunia Advisory, SA12557, September 16, 2004 Fedora Update Notification, FEDORA-2004-303, September 21, 2004 Gentoo Linux Security Advisory, GLSA 200409-24, September 17, 2004 Sun(sm) Alert Notification, 57646, October 7, 2004 Conectiva Linux Security Announcement, CLA-2004:880, October 26, 2004 **Fedora Legacy Update Advisory, FLSA:2076, November 5, 2004**

Multiple Vendors LVM Logical Volume Management Utilities 1.0.4, 1.0.7, 1.0.8	A vulnerability exists due to the insecure creation of temporary files, which could possibly let a malicious user overwrite arbitrary files. Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/l/lvm10/** **Debian:** **http://security.debian.org/pool/updates/main/l/lvm10/** There is no exploit code required.	Trustix LVM Utilities Insecure Temporary File Creation CVE Name: CAN-2004-0972	Medium	Trustix Secure Linux Bugfix Advisory, TSL-2004-0050, September 30, 2004 **Ubuntu Security Notice, USN-15-1, November 1, 2004** **Debian Security Advisory, DSA 583-1, November 3, 2004**

Multiple Vendors OpenBSD 3.4, 3.5; SuSE Linux 8.1, 8.2, 9.0, x86_64, 9.1, Linux Enterprise Server 9, 8; X.org X11R6 6.7.0, 6.8; XFree86 X11R6 3.3.6, 4.0, 4.0.1, 4.0.2 -11, 4.0.3, 4.1 .0, 4.1 -12, 4.1 -11, 4.2 .0, 4.2.1, Errata, 4.3.0; **Avaya Intuity LX, MN100, Modular Messaging (MSS) 1.1, 2.0**	Multiple vulnerabilities exist: a stack overflow vulnerability exists in 'xpmParseColors()' in 'parse.c' when a specially crafted XPMv1 and XPMv2/3 file is submitted, which could let a remote malicious user execute arbitrary code; a stack overflow vulnerability exists in the 'ParseAndPutPixels()' function in -create.c' when reading pixel values, which could let a remote malicious user execute arbitrary code; and an integer overflow vulnerability exists in the colorTable allocation in 'xpmParseColors()' in 'parse.c,' which could let a remote malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/i/imlib/ Mandrake: http://www.mandrakesecure.net/en/ftp.php OpenBSD: ftp://ftp.OpenBSD.org/pub/OpenBSD/patches/ SuSE: ftp://ftp.suse.com/pub/suse/ X.org: http://x.org/X11R6.8.1/ Gentoo: http://security.gentoo.org/glsa/glsa-200409-34.xml IBM: http://www-912.ibm.com/eserver/support/fixes/fcgui.jsp RedHat: http://rhn.redhat.com/errata/RHSA-2004-478.html Avaya: http://support.avaya.com/japple/css/japple?temp.groupID=128450&temp.selectedFamily=128451&temp.selectedProduct=154235&temp.selectedBucket=126655&temp.feedbackState=askForFeedback&temp.documentID=203389& PAGE=avaya.css.CSSLvl1Detail&executeTransaction=avaya.css.UsageUpdate() Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57652-1&searchclause= **Mandrake: http://www.mandrakesoft.com/security/advisories**	LibXpm Image Decoding Multiple Remote Buffer Overflow CVE Names: CAN-2004-0687 CAN-2004-0688	High	X.Org Foundation Security Advisory, September 16, 2004 US-CERT Vulnerability Notes, VU#537878 & VU#882750, September 30, 2004 SecurityFocus, October 4, 2004 SecurityFocus, October 18, 2004 Sun(sm) Alert Notification, 5765, October 18, 2004 **Mandrakelinux Security Update Advisory, MDKSA-2004:124, November 2, 2004**

MySQL AB MySQL 3.20 .x, 3.20.32 a, 3.21 .x, 3.22 .x, 3.22.26-3.22.30, 3.22.32, 3.23 .x, 3.23.2-3.23.5, 3.23.8-3.23.10, 3.23.22-3.23.34, 3.23.36-3.23.56, 3.23.58, 4.0.0-4.0.15, 4.0.18, 4.0.20, 4.1 .0-alpha, 4.1 .0-0, 4.1.2 -alpha, 4.1.3 -beta, 4.1.3 -0, 5.0 .0-alpha, 5.0 .0-0	A buffer overflow vulnerability exists in the 'mysql_real_connect' function due to insufficient boundary checking, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code. *Note: Computers using glibc on Linux and BSD platforms may not be vulnerable to this issue.* Debian: http://security.debian.org/pool/updates/main/m/mysql/ Trustix: http://http.trustix.org/pub/trustix/updates/ OpenPKG: ftp://ftp.openpkg.org/release/ **Mandrake: http://www.mandrakesoft.com/security/advisories** We are not aware of any exploits for this vulnerability.	MySQL Mysql_real_connect Function Remote Buffer Overflow CVE Name: CAN-2004-0836	High/Low (Low if a DoS)	Secunia Advisory, SA12305, August 20, 2004 Debian Security Advisory, DSA 562-1, October 11, 2004 Trustix Secure Linux Security Advisory, TSLSA-2004-0054, October 15, 2004 **Mandrakelinux Security Update Advisory, MDKSA-2004:119, November 1, 2004**

MySQL AB MySQL 3.23.49, 4.0.20	A vulnerability exists in the 'mysqlhotcopy' script due to predictable files names of temporary files, which could let a malicious user obtain elevated privileges. Debian: http://security.debian.org/pool/updates/main/m/ Gentoo: http://security.gentoo.org/glsa/glsa-200409-02.xml SuSE: ftp://ftp.suse.com/pub/suse/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-569.html OpenPKG: ftp://ftp.openpkg.org/release/ **Mandrake: http://www.mandrakesoft.com/security/advisories** There is no exploit code required.	MySQL 'Mysqlhotcopy' Script Elevated Privileges CVE Name: CAN-2004-0457	Medium	Debian Security Advisory, DSA 540-1, August 18, 2004 Gentoo Linux Security Advisory GLSA 200409-02, September 1, 2004 SUSE Security Announcement, SUSE-SA:2004:030, September 6, 2004 RedHat Security Advisory, ,RHSA-2004:569-16, October 20, 2004 **Mandrakelinux Security Update Advisory, MDKSA-2004:119, November 1, 2004**

MySQL AB MySQL 3.x, 4.x	Two vulnerabilities exist: a vulnerability exists due to an error in 'ALTER TABLE ... RENAME' operations because the 'CREATE/INSERT' rights of old tables are checked, which potentially could let a remote malicious user bypass security restrictions; and a remote Denial of Service vulnerability exists when multiple threads issue 'alter' commands against 'merge' tables to modify the 'union.' Updates available at: http://dev.mysql.com/downloads/mysql/ Debian: http://security.debian.org/pool/updates/main/m/mysql Trustix: http://http.trustix.org/pub/trustix/updates/ **Mandrake: http://www.mandrakesoft.com/security/advisories** We are not aware of any exploits for these vulnerabilities.	MySQL Security Restriction Bypass & Remote Denial of Service CVE Names: CAN-2004-0835, CAN-2004-0837	Low/ Medium (Low if a DoS; and Medium if security restrictions can be bypassed)	Secunia Advisory, SA12783, October 11, 2004 Trustix Secure Linux Security Advisory, TSLSA-2004-0054, October 15, 2004 **Mandrakelinux Security Update Advisory, MDKSA-2004:119, November 1, 2004**

Netatalk Netatalk Open Source Apple File Share Protocol Suite 1.5 pre6, 1.6.1, 1.6.4	A vulnerability exists due to the insecure creation of temporary files, which could possibly let a malicious user overwrite arbitrary files. Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200410-25.xml **Mandrake: http://www.mandrakesoft.com/security/advisories** There is no exploit code required.	NetaTalk Insecure Temporary File Creation CVE Name: CAN-2004-0974	Medium	Trustix Secure Linux Bugfix Advisory, TSL-2004-0050, September 30, 2004 Gentoo Linux Security Advisory GLSA 200410-25, October 25, 2004 **Mandrakelinux Security Update Advisory, MDKSA-2004:121, November 2, 2004**
PostgreSQL PostgreSQL 7.0.2, 7.0.3, 7.1-7.1.3, 7.2-7.2.4, 7.3-7.3.4, 7.4, 7.4.3, 7.4.5	A vulnerability exists in the RPM initialization script. The impact was not specified. No workaround or patch available at time of publishing. We are not aware of any exploits for this vulnerability.	PostgreSQL Unspecified RPM Initialization Script	Not Specified	SecurityFocus, November 1, 2004

proxytunnel proxytunnel 1.0.6, 1.1.3, 1.2.0, 1.2.2	A format string vulnerability exists in the 'message()' function in 'messages.c' when running in daemon mode, which could let a remote malicious user execute arbitrary code. Upgrade available at: http://sourceforge.net/project/showfiles.php?group_id=39840 Gentoo: http://security.gentoo.org/glsa/glsa-200411-07.xml We are not aware of any exploits for this vulnerability.	Proxytunnel Remote Format String	High	Gentoo Linux Security Advisory, GLSA 200411-07, November 3, 2004
Qwikmail Qwikmail 0.3	A vulnerability exists due to a format string error in 'qwik-smtpd.c,' which could let a remote malicious user execute arbitrary code. Patch available at: http://qwikmail.sourceforge.net/smtpd/qwik-smtpd-0.3.patch **An exploit script has been published.**	QwikMail Format String	High	Secunia Advisory, SA13037, November 1, 2004 **Packetstorm, November 10, 2004**

Rob Flynn Gaim 0.10 x, 0.10.3, 0.50-0.75	Multiple vulnerabilities exist which could let a remote malicious user execute arbitrary code or cause a Denial of Service: a vulnerability exists during the installation of a smiley theme; a heap overflow vulnerability exists when processing data from a groupware server; a buffer overflow vulnerability exists in the URI parsing utility; a buffer overflow vulnerability exists when performing a DNS query to obtain a hostname when signing on to zephyr; a buffer overflow vulnerability exists when processing Rich Text Format (RTF) messages; and a buffer overflow vulnerability exists in the 'content-length' header when an excessive value is submitted. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo:http://security.gentoo.org/glsa/glsa-200408-27.xml Rob Flynn: http://sourceforge.net/project/showfiles.php?group_id=235&package_id=253&release_id=263425 Slackware: ftp://ftp.slackware.com/pub/slackware/slackware-10.0/patches/packages/gaim-0.82-i486-1.tgz Fedora Legacy: http://download.fedoralegacy.org/redhat/ Mandrake: http://www.mandrakesecure.net/en/ftp.php **Conectiva: ftp://atualizacoes.conectiva.com.br/10/** We are not aware of any exploits for these vulnerabilities.	Gaim Multiple Vulnerabilities CVE Names: CAN-2004-0784 CAN-2004-0754 CAN-2004-0785	Low/High (High if arbitrary code can be executed)	SecurityFocus, August 26, 2004 Fedora Legacy Update Advisory, FLSA:1237, October 16, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:110, October 21, 2004 **Conectiva Linux Security Announcement, CLA-2004:884, November 4, 2004**

Sophos MailMonitor for SMTP 2.1	A vulnerability exists when handling malformed email messages. The impact was not specified. Updates available at: http://www.sophos.com/sophos/products/full/mmsmtp-linux-update.tar.gz http://www.sophos.com/sophos/products/full/mmsmtp-solaris-update.tar.Z We are not aware of any exploits for this vulnerability.	Sophos MailMonitor SMTP Email Handling	Not Specified	Sophos Support Knowledgebase Article, November 5, 2004
SpamAssassin SpamAssassin 3.0.1	A remote Denial of Service vulnerability exists when a malicious user submits a specially crafted email message that contains several domain addresses in the email body. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	SpamAssassin Remote Denial of Service	Low	SecurityTracker Alert ID, 1012071, November 3, 2004

Squid-cache.org Debian Fedora Gentoo Mandrake OpenPKG RedHat SGI SuSE Tinysofa Trustix Squid Web Proxy Cache 2.0 PATCH2, 2.1 PATCH2, 2.3 STABLE5, 2.4 STABLE7, 2.4.2.5 STABLE5, STABLE4, STABLE3, STABLE1	A buffer overflow vulnerability exists in 'helpers/ntlm_auth/SMB/libntlmssp.c' in the 'ntlm_check_auth()' function due to insufficient validation, which could let a remote malicious user execute arbitrary code. Patches available at: http://www.squid-cache.org/~wessels/patch/libntlmssp.c.patch Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200406-13.xml Mandrake: http://www.mandrakesoft.com/security/advisories RedHat: http://rhn.redhat.com/errata/RHSA-2004-242.html SGI: ftp://patches.sgi.com/support/free/security/advisories/ SuSE: ftp://ftp.suse.com/pub/suse/ Tinysofa: http://http.tinysofa.org/pub/tinysofa/updates/server-1.0/rpms/squid-2.5.STABLE5-6ts.i586.rpm Trustix: http://http.trustix.org/pub/trustix/updates/ **Conectiva: ftp://atualizacoes.conectiva.com.br/** Exploit script has been published.	Squid Proxy NTLM Buffer Overflow CVE Name: CAN-2004-0541	High	Fedora Update Notifications, FEDORA-2004-163 & 164, June 9, 2004 Gentoo Linux Security Advisory, GLSA 200406-13, June 17, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:059, June 9, 2004 RedHat Security Advisory, RHSA-2004:242-06, June 9, 2004 SGI Security Advisory, 20040604-01-U, June 21, 2004 SUSE Security Announcement, SuSE-SA:2004:016, June 9, 2004 Tinysofa Security Advisory, TSSA-2004-010, June

Squid-cache.org Squid 2.5-STABLE6, 3.0-PRE3-20040702; when compiled with SNMP support	A remote Denial of Service vulnerability exists in the 'asn_parse_header()' function in 'snmplib/asn1.c' due to an input validation error when handling certain negative length fields. Updates available at: http://www.squid-cache.org/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Gentoo: http://security.gentoo.org/glsa/glsa-200410-15.xml Trustix: http://http.trustix.org/pub/trustix/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-591.html Mandrake: http://www.mandrakesecure.net/en/ftp.php Debian: http://security.debian.org/pool/updates/main/s/squid/ OpenPKG: ftp://ftp.openpkg.org/release/ **Conectiva: ftp://atualizacoes.conectiva.com.br/** **Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/s/squid/** We are not aware of any exploits for this vulnerability.	Squid Remote Denial of Service CVE Name: CAN-2004-0918	Low	iDEFENSE Security Advisory, October 11, 2004 Fedora Update Notification, FEDORA-2004-338, October 13, 2004 Trustix Secure Linux Security Advisory, TSLSA-2004-0054, October 15, 2004 Gentoo Linux Security Advisory, GLSA 200410-15, October 18, 2004 RedHat Security Advisory, RHSA-2004:591-04, October 20, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:112, October 21, 2004

Squid-cache.org Squid Web Proxy Cache 2.0 PATCH2, 2.1 PATCH2, 2.3 STABLE5, 2.4, STABLE7, 2.5 STABLE1-STABLE6, Squid Web Proxy Cache 3.0 PRE1-PRE3	A remote Denial of Service vulnerability exists in 'lib/ntlmauth.c' due to insufficient validation of negative values in the 'ntlm_fetch_string()' function. Patches available at: http://www1.uk.squid-cache.org/squid/Versions/v2/2.5/bugs/squid-2.5.STABLE6-ntlm_fetch_string.patch Gentoo: http://security.gentoo.org/glsa/glsa-200409-04.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Trustix: http://http.trustix.org/pub/trustix/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-462.html TurboLinux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/ **Conectiva: ftp://atualizacoes.conectiva.com.br/** **Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/s/squid/** We are not aware of any exploits for this vulnerability.	Squid Proxy NTLM Authentication Remote Denial of Service CVE Name: CAN-2004-0832	Low	Secunia Advisory, SA12444, September 3, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:093, September 15, 2004 Trustix Secure Linux Security Advisory, TSLSA-2004-0047, September 16, 2004 RedHat Security Advisory, RHSA-2004:462-10, September 30, 2004 Turbolinux Security Announcement, October 5, 2004 **Conectiva Linux Security Announcement, CLA-2004:882, November 3, 2004**

Subversion Subversion 1.0-1.0.7, 1.1 .0 rc1-rc3	A vulnerability exists in the 'mod_authz_svn' module due to insufficient restricted access to metadata on unreadable paths, which could let a remote malicious user obtain sensitive information. Update available at: http://subversion.tigris.org/tarballs/subversion-1.0.8.tar.gz Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Gentoo: http://security.gentoo.org/glsa/glsa-200409-35.xml **Conectiva: ftp://atualizacoes.conectiva.com.br/10/** There is no exploit code required.	Subversion Mod_Authz_Svn Metadata Information Disclosure CVE Name: CAN-2004-0749	Medium	SecurityTracker Alert ID, 1011390, September 23, 2004 Gentoo Linux Security Advisory, GLSA 200409-35, September 29, 2004 **Conectiva Linux Security Announcement, CLA-2004:883, November 4, 2004**
Technote Technote	A vulnerability exists in the 'main.cgi' script due to insufficient validation of user-supplied input in the 'file name' parameter, which could let a remote malicious user execute arbitrary commands. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Technote 'main.cgi' Input Validation	High	SecurityTracker Alert I,: 1012117, November 8, 2004

Tomasz Kloczko Shadow 4.0-4.0.4	A vulnerability exists in the in the 'chfn' and 'chsh' utilities due to insufficient sanitization of user-supplied input, which could let a remote malicious user bypass authentication. Upgrades available at : ftp://ftp.pld.org.pl/software/shadow/shadow-4.0.5.tar.gz **Gentoo:** **http://security.gentoo.org/glsa/glsa-200411-09.xml** We are not aware of any exploits for this vulnerability.	Shadow Authentication Bypass	Medium	SecurityFocus, October 28, 2004 **Gentoo Linux Security Advisory, GLSA 200411-09, November 4, 2004**

xmlsoft.org Libxml2 2.6.12-2.6.14	Multiple buffer overflow vulnerabilities exist: a vulnerability exists in the 'xmlNanoFTPScanURL()' function in 'nanoftp.c' due to a boundary error, which could let a remote malicious user execute arbitrary code; a vulnerability exists in the 'xmlNanoFTPScanProxy()' function in 'nanoftp.c,' which could let a remote malicious user execute arbitrary code; and a vulnerability exists in the handling of DNS replies due to various boundary errors, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://xmlsoft.org/sources/libxml2-2.6.15.tar.gz OpenPKG: ftp://ftp.openpkg.org/release/2.1/UPD/libxml-2.6.11-2.1.1.src.rpm Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ **Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/** **Gentoo:** **http://security.gentoo.org/glsa/glsa-200411-05.xml** **Mandrake: http://www.mandrakesoft.com/security/advisories** **OpenPKG: ftp://ftp.openpkg.org/release/** **Trustix:** **http://www.trustix.org/errata/2004/0055/** **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/libx/libxml2/** An exploit script has been published.	Libxml2 Multiple Remote Stack Buffer Overflows CVE Name: CAN-2004-0989	High	SecurityTracker Alert I, : 1011941, October 28, 2004 **Fedora Update Notification, FEDORA-2004-353, November 2, 2004** **Gentoo Linux Security Advisory, GLSA 200411-05, November 2,2 004** **Mandrakelinux Security Update Advisory, MDKSA-2004:127, November 4, 2004** **OpenPKG Security Advisory, OpenPKG-SA-2004.050, November 1, 2004** **Trustix Secure Linux Security Advisory,**

ychat.org yChat 0.1-0.6	A remote Denial of Service vulnerability exists due to some security issues when processing HTTP connections. Upgrades available at: http://ftp.buetow.org/pub/yChat/CPP-yChat/ychat-0.7.tar.bz2 We are not aware of any exploits for this vulnerability.	yChat HTTP Remote Denial of Service	Low	SecurityTracker Alert ID, 1012043, November 2, 2004
Yukihiro Matsumoto Ruby 1.8.x	A remote Denial of Service vulnerability exists due to an input validation error in 'cgi.rb.' Debian: http://security.debian.org/pool/updates/main/r/ruby Mandrake: http://www.mandrakesoft.com/security/advisories Currently we are not aware of any exploits for this vulnerability.	Ruby Infinite Loop Remote Denial of Service CVE Name: CAN-2004-0983	Low	Secunia Advisory, SA13123, November 8, 2004
Zile Zile Text Editor 1.4, 1.5-1.5.3, 1.6-1.6.2, 1.7 b1-b3	Several potential buffer overflows exist, which could possibly let a remote malicious user execute arbitrary code. Upgrades available at: http://prdownloads.sourceforge.net/zile/zile-2.0-a1.tar.gz?download We are not aware of any exploits for these vulnerabilities.	Zile Buffer Overflows	High	SecurityTracker Alert ID, 1012080, November 4, 2004

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
Brandon Tallent AntiBoard 0.7.3	An input validation vulnerability exists due to insufficient sanitization of user-supplied input prior to including it in an SQL query, which could let a remote malicious user execute arbitrary SQL commands. No workaround or patch available at time of publishing. There is no exploit code required.	AntiBoard Input Validation	High	SecurityTracker Alert ID, 1012076, November 4, 2004

Cisco Systems IOS R12.x, 12.x	A remote Denial of Service vulnerability exists when a malicious user submits a specially crafted TCP connection to a telnet or reverse telnet port. Potential workarounds available at: http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml We are not aware of any exploits for this vulnerability.	Cisco IOS Telnet Service Remote Denial of Service	Low	Cisco Security Advisory, cisco-sa-20040827, August 27, 2004 US-CERT Vulnerability Note VU#384230 Cisco Security Advisory, 61671 Rev 2.2, October 20, 2004 **Cisco Security Advisory, 61671 Rev 2.3, October 31, 2004**
eGroupWare.org eGroupWare prior to 1.0.00.006	A Directory Traversal vulnerability exists in 'JiNN' due to insufficient validation of user-supplied input, which could let a remote malicious user obtain sensitive information. Update available at: http://sourceforge.net/project/showfiles.php?group_id=78745 We are not aware of any exploits for this vulnerability.	eGroupWare JiNN Directory Traversal	Medium	Secunia Advisory, SA13110, November 8, 2004

Gallery Project Gallery 1.4 -pl1&pl2, 1.4, 1.4.1, 1.4.2, 1.4.3 -pl1 & pl2; Gentoo Linux	A Cross-Site Scripting vulnerability exists in several files, including 'view_photo.php,' 'index.php,' and 'init.php' due to insufficient input validation, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://sourceforge.net/project/showfiles.php?group_id=7130 Gentoo: http://security.gentoo.org/glsa/glsa-200411-10.xml There is no exploit code required.	Gallery Cross-Site Scripting	High	Gentoo Linux Security Advisory, GLSA 200411-10:01, November 6, 2004
gallery.devrandom.org.uk FsPHPGallery 0.2, 0.3.1, 1.0.1, 1.1	Multiple vulnerabilities exist: a Denial of Service vulnerability exists due to an input validation error when resizing images; and a vulnerability exists in 'index.php' due to insufficient verification of input passed to the 'dir' parameter, which could let a malicious user obtain sensitive information. Upgrades available at: http://gallery.devrandom.org.uk/releases/fsphpgallery-1.2.tar.gz There is no exploit code required.	FsPHPGallery Multiple Input Validation	Low/ Medium (Medium if sensitive information can be obtained)	Secunia Advisory, SA13074, November 3, 2004

Gbook MX Gbook MX 2.0, 3.0, 4.1	Multiple unspecified SQL injection vulnerabilities exist due to insufficient sanitization of user-supplied input prior to including it in SQL queries, which could let a remote malicious user compromise the application, disclosure or modify data, or permit the exploitation of vulnerabilities in the underlying database implementation. Upgrades available at: http://sourceforge.net/project/showfiles.php?group_id=80296&package_id=123432&release_id=279828 We are not aware of any exploits for these vulnerabilities.	Gbook MX Multiple Unspecified SQL Injection	Medium	SecurityFocus, November 3, 2004
Goollery Goollery 0.3	Multiple Cross-Site Scripting vulnerabilities due to insufficient sanitization of user-supplied input, exists which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Goollery Multiple Cross-Site Scripting	High	SecurityFocus, November 2, 2004
Moodle moodle 1.1.1, 1.2, 1.2.1, 1.3-1.3.4, 1.4.1, 1.4.2	A vulnerability exists in the 'glossary' module due to insufficient verification of user-supplied input, which could let a remote malicious user execute arbitrary SQL code. Update available at: http://moodle.org/download/ There is no exploit code required.	Moodle Remote Glossary Module SQL Injection	High	Secunia Advisory, SA13091, November 5, 2004

Multiple Vendors Archive::Zip 1.13, F-Secure Anti-Virus for Microsoft Exchange 6.30, 6.30 SR1, and 6.31, Computer Associates, Eset, Kaspersky, McAfee, Sophos, RAV	Remote exploitation of an exceptional condition error in multiple vendors' anti-virus software allows malicious users to bypass security protections by evading virus detection. The problem specifically exists in the parsing of .zip archive headers. This vulnerability affects multiple anti-virus vendors including McAfee, Computer Associates, Kaspersky, Sophos, Eset and RAV. Instructions for Computer Associates, Eset, Kaspersky, McAfee, Sophos, and RAV are available at: http://www.idefense.com/application/poi/display?id=153&type=vulnerabilities&flashstatus=true **Gentoo:** **http://security.gentoo.org/glsa/glsa-200410-31.xml** **Mandrakelinux 10.1 and Mandrakelinux 10.1/X86_64:** **http://www.mandrakesoft.com/security/advisories** **A fix for F-Secure is available at::** **ftp://ftp.f-secure.com/support/hotfix/fsav-mse/fsavmse63x-02.zip** Proofs of Concept exploits have been published.	Multiple Vendor Anti-Virus Software Detection Evasion CVE Names: CAN-2004-0932 CAN-2004-0933 CAN-2004-0934 CAN-2004-0935 CAN-2004-0936 CAN-2004-0937	High	iDEFENSE Security Advisory, October 18, 2004 Secunia Advisory ID: SA13038, November 1, 2004 **SecurityFocus, Bugtraq ID: 11448, November 2, 2004** **SecurityTracker Alert ID: 1012057, November 3, 2004**

Multiple Vendors Microsoft Internet Explorer 6, Microsoft Outlook Express 6, **Apple Safari 1.2.3 (v125.9)**	**Multiple web browsers do not properly display the location of HTML documents in the status bar. An attacker could exploit this behavior to mislead users into revealing sensitive information.** This vulnerability was confirmed in Internet Explorer SP1 but not SP2. A Proof of Concept exploit has been published.	**Multiple Web Browsers TABLE Elements Interpretation**	Medium	Secunia Advisory, SA13015, October 29, 2004 **US-CERT Vulnerability Notes VU#925430 & VU#702086, November 4, 2004**
Multiple Vendors Microsoft Internet Explorer 6.0 **Apple Safari 1.2.3 (v125.9)**	**Multiple browsers are prone to a remote Denial of Service vulnerability. The issue presents itself due to a malfunction that occurs when certain font tags are encountered and rendered. When a page that contains the malicious HTML code is viewed, the browser will crash.** No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	**Multiple Web Browsers Font Tag Denial Of Service**	Low	SecurityFocus Bugtraq ID, 11536, October 26, 2004 **US-CERT, Vulnerability Note VU#925430, November 4, 2004**
NetGear ProSafe Dual Band Wireless VPN Firewall FWAG114	A vulnerability exists because a default community string is used for SNMP, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required.	NetGear ProSafe Dual Band Wireless VPN Firewall Default SNMP Community String	Medium	SecurityFocus, November 2, 2004

paystream.sourceforge.net AudienceConnect SecureEditor	A vulnerability exists in the IP address-based access control feature, which could let a remote unauthorized malicious user obtain access. Update available at: http://sourceforge.net/project/showfiles.php?group_id=98629&package_id=132849 We are not aware of any exploits for this vulnerability.	AudienceConnect SecureEditor Unauthorized Access	Medium	SecurityTracker Alert ID, 1012066, November 3, 2004
Pierre Chifflier wzdftpd prior to 0.4.3	A remote Denial of Service vulnerability exists because ident connections are not properly closed. Update available at: http://sourceforge.net/project/showfiles.php?group_id=78247 We are not aware of any exploits for this vulnerability.	Pierre Chifflier wzdftpd ident Processing Remote Denial of Service	Low	SecurityTracker Alert ID, 1012078, November 4, 2004
Sun Microsystems, Inc. Java System Application Server 7.0 Standard Edition, Platform Edition, 7.0 2004Q2, Java System Web Server 6.0, SP1-SP7, 6.1, SP1	A remote Denial of Service vulnerability exists due to a failure to process malformed client certificates. Patches available at: http://wwws.sun.com/software/download/products/40968fe6.html There is no exploit code required.	Sun Java System Web & Application Servers Remote Denial of Service	Low	Sun(sm) Alert Notification, 57669, November 2, 2004

Sun Microsystems, Inc. Java System Application Server 7.0 Standard Edition, Platform Edition, 7.0 2004Q2	A vulnerability exists in the processing of HTTP TRACE requests, which could let a remote malicious user obtain sensitive information. Workaround available at: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57670-1 There is no exploit code required.	Sun Java System Application Server HTTP TRACE Information Disclosure	Medium	Sun(sm) Alert Notification, 57670, November 2, 2004

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. The "Workaround or Patch Available" column indicates if vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have published workarounds or patches.

Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script name	Workaround or Patch Available	Script Description
November 10, 2004	qwik_fmtstr_xpl.c	Yes	Script that exploits the QwikMail Format String vulnerability.
November 8, 2004	WPA Cracker	N/A	Proof of Concept exploit for the Wi-Fi Protected Access encryption algorithm weakness.
November 6, 2004	602res.zip	Yes	Exploit for the Software602 602 LAN Suite Multiple Remote Denial Of Service vulnerabilities.
November 5, 2004	iptablesDoS.c	Yes	Proof of Concept Denial of Service exploit for the Linux Kernel IPTables Logging Rules Remote Denial

			of Service vulnerability.
November 5, 2004	wX.tar.gz	N/A	A kernel based rootkit for Mac OSX which is roughly based on adore. It runs as a kernel extension, similar to a LKM. Requires Xcode.
November 4, 2004	InternetExploiter.html.gz	No	Script that exploits the Microsoft Internet Explorer Malformed IFRAME Remote Buffer Overflow vulnerability.

Trends

- A new phishing attack is utilizing a vulnerability in Internet Explorer, patched early this year, to hide its true source. The attack, called Citifraud.A takes the form of a Web page or HTML e-mail. It has no means of self-propagation. The page or e-mail appears to come from a bank and contains a link that appears to go to the bank Web site. The link uses a vulnerability in Internet Explorer that causes the browser to improperly display the URL of the Web site due to a flaw in a process called canonicalization. For more information, see http://www.eweek.com/article2/0,1759,1713548,00.asp.
- Malicious software cases rose 22 percent in October, with Trojan horses accounting for nearly half, according to a newly released report by security company Trend Micro's TrendLabs. For more information see: http://news.zdnet.com/2100-1009_22-5438228.html.

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trends	Date
1	Netsky-P	Win32 Worm	Stable	March 2004
2	Zafi-B	Win32 Worm	Stable	June 2004
3	Netsky-Z	Win32 Worm	Stable	April 2004
4	Netsky-D	Win32 Worm	Stable	March 2004
5	Bagle-AA	Win32 Worm	Stable	April 2004
6	Netsky-B	Win32 Worm	Stable	February 2004
7	Netsky-Q	Win32 Worm	Stable	March 2004
8	Bagle-Z	Win32 Worm	Stable	April 2004
9	Bagle.AT	Win32 Worm	Stable	October 2004
10*	Netsky-C	Win32 Worm	Stable	February 2004
10*	Bagle-AI	Win32 Worm	Return to Table	July 2004

Table Updated November 9, 2004

* Netsky-C and Bagle-AI tied for the last spot in the Top 10. Bagle-AI returns to the table after remaining relatively stable just off the Top 10 for the past several weeks.

Viruses or Trojans Considered to be a High Level of Threat

- MyDoom.AG: A new computer worm emerged on Tuesday, November 9, which swiftly capitalized on the announcement of a security vulnerability in

Microsoft's Internet Explorer to a full-blown virus that spreads in the wild. The vulnerability was discovered and made public on Friday, November 5. Microsoft said the worm is a variant of MyDoom and that it was investigating the threat the worm poses. Some anti-virus companies said the new worm was different from MyDoom because it spreads via weblinks and not e-mail attachments. Microsoft said that consumers who had installed Service Pack 2 for Windows XP were at a reduced risk. The weakness in Internet Explorer is known as the IFRAME buffer overflow vulnerability. (Reuters, November 9, 2004)

The following table provides, in alphabetical order, a list of new viruses, variations of previously encountered viruses, and Trojans that have been discovered during the period covered by this bulletin. This information has been compiled from the following anti-virus vendors: Sophos, Trend Micro, Symantec, McAfee, Network Associates, Central Command, F-Secure, Kaspersky Labs, MessageLabs, Panda Software, Computer Associates, and The WildList Organization International. Users should keep anti-virus software up to date and should contact their anti-virus vendors to obtain specific information on the Trojans and Trojan variants that anti-virus software detects.

NOTE: At times, viruses and Trojans may contain names or content that may be considered offensive.

Name	Aliases	Type
Backdoor.Alcani		Trojan
Backdoor.Alnica		Trojan
Backdoor.Hacarmy.F		Trojan
Backdoor.IRC.Bifrut		Trojan
Bagz.F	I-Worm.Bagz.f I-Worm.Bagz.g W32.Bagz.H@mm W32/Bagz-F W32/Bagz.gen@MM Win32.Bagz.F Win32.Bagz.F!ZIP Win32/Bagz.166913.Worm WORM_BAGZ.F	Win32 Worm
Bagz.H	W32/Bagz.H.worm	Win32 Worm
Citifraud.A	Trj/Citifraud.A	Trojan
JS/QHosts21-A		Trojan
Mitglieder.AY	W32/Mitglieder.AY.worm	Win32 Worm
Mydoom.AG	I-Worm.Mydoom.ab I-Worm.Mydoom.ad	Win32 Worm

	MyDoom.AF MyDoom.AG W32.Mydoom.AI@mm W32/Bofra-A W32/Bofra-C W32/Mydoom.ag@M W32/Mydoom.ag@MM W32/Mydoom.AJ@mm Win32.Mydoom.AF Win32/Mydoom.AE Win32/Mydoom.AJ WORM_MYDOOM.AG WORM_MYDOOM.AI	
Mydoom.AH	I-Worm.Mydoom.ad W32.Mydoom.AH@mm W32/Bofra-B W32/Mydoom.ah@MM Win32.Mydoom.AG Win32/Mydoom.AH@mm WORM_MYDOOM.AH	Win32 Worm
Troj/Bancban-AC	W32/Forbot-CD	Win32 Worm
Troj/StartPa-DO		Win32 Worm
Trojan.Beagooz.B		Trojan
Trojan.Beagooz.C		Trojan
VBS.Midfin@mm	I-Worm.SMWF.a	Visual Basic Virus
W32.Gaobot.BQJ	Backdoor.Win32.Agobot.gen	Win32 Worm
W32.Josam.Worm		Win32 Worm
W32.Linkbot.A	Backdoor.Win32.Rbot.dc	Win32 Worm
W32.Orpheus.A		Win32 Worm
W32.Randex.BTB		Win32 Worm
W32.Shodi.D		Win32 Worm
W32/Bagz-F	W32/Bagz.gen@MM	Win32 Worm
W32/Bofra-A	W32/Mydoom.ag@M	Win32 Worm
W32/Famus-F	I-Worm.Famus.c W32/Bilb.worm WORM_LIBR.A	Win32 Worm
W32/Forbot-CD	Backdoor.Win32.Wootbot.gen	Win32 Worm
W32/Forbot-CF		Win32 Worm
W32/Rbot-OV		Win32 Worm
W32/Rbot-OX	Backdoor.Win32.Rbot.gen	Win32 Worm

	W32/Sdbot.worm.gen.i	
W32/Rbot-OY		Win32 Worm
W32/Rbot-PA	Backdoor.Win32.Rbot.gen	Win32 Worm
W32/Rbot-PC	Backdoor.Win32.Rbot.gen W32/Sdbot.worm.gen.i WORM_SPYBOT.GZ	Win32 Worm
W32/Rbot-PE	Backdoor.Win32.Wootbot.gen	Win32 Worm
W32/Rbot-PG	W32/Sdbot.worm.gen.t	Win32 Worm
W32/Sdbot-QX	Backdoor.Win32.SdBot.gen	Win32 Worm
Worm/Agobot.PD	WORM_AGOBOT.AAN	Win32 Worm
X97M.Avone.A	Macro.Excel97.Viki.a	MS Excel Virus